On short digital signatures with Eulerian transformations

Vasyl Ustymenko[1,2]

[1] *Royal Holloway University of London, United Kingdom.*
[2] *Institute of telecommunications and global information space, Kyiv, Ukraine*
E - mail: Vasyl.Ustymenko@rhul.ac.uk

Abstract. Let n stands for the length of digital signatures with quadratic multivariate public rule in n variables. We construct postquantum secure procedure to sign $O(n^t)$, $t \geq 1$ digital documents with the signature of size n *in time* $O(n^{3+t})$. It allows to sign $O(n^t)$, $t < 1$ in time $O(n^4)$. The procedure is defined in terms of Algebraic Cryptography. Its security rests on the semigroup based protocol of Noncommutative Cryptography referring to complexity of the decomposition of the collision element into composition into given generators. The protocol uses the semigroup of Eulerian transformations of variety $(K^*)^n$ where K^* is a nontrivial multiplicative group of the finite commutative ring K. Its execution complexity is $O(n^3)$. Additionally we use this protocol to define asymmetric cryptosystem with the space of plaintexts and ciphertexts $(K^*)^n$ which allows users to encrypt and decrypt $O(n^t)$ documents of size n in time $O(n^{3+[t]})$ where $[x]$ stands for the flow function from x. Finally we suggest protocol based cryptosystem working with plaintext space $(K^*)^n$ and the space of ciphertext K^n which allows decryption of $O(n^t)$, $t>1$ documents of size n in time $O(n^{t+3})$, $t>1$. The multivariate encryption map has linear degree $O(n)$ and density $O(n^4)$. We discuss the idea of public key with Eulerian transformations which allows to sign $O(n^t)$, $t \geq 0$ documents in time $O(n^{t+2})$. The idea of delivery and usage of several Eulerian and quadratic transformations is also discussed.

Keywords: Multivariate Cryptography, Digital signatures, Noncommutative Cryptography, Eulerian transformations , Protocol based cryptosystems, Public keys.

1. Introduction.

Let us discuss the question about group or semigroups which are useful for Cryptography. Specialist working in Noncommutative Cryptography may refer to Thompson or Grigorchuk groups, braids group or affine Cremona semigroups, but most of other cryptographers will mention cyclic groups or monogenic semigroups. One can see that RSA cryptosystem uses cyclic subgroup of Z_{pq}, Diffie Hellman protocol uses cyclic F^*_p. if we have some encryption public rule acting bijectively on the space of plaintext it is generating corresponding cyclic group. If the public rule is not bijective then it is generating of some monogenic semigroup of large order with some large index.

Noteworthy that the complexity of investigation the cyclic group depends heavily on the way its presentation in the memory of computer. In the case of F^*_p for large prime p we have discrete logarithm problem but in the case of additive group of Z_{p-1} we have just a diophantine equation. Recall that formal Diffie Hellman protocol can

be established for each finite monogenic semigroup and the cryptanalytic studies of the semigroup case has to be continued.

In this paper we present some short digital signatures algorithms with the use of Eulerian transformations of affine spaces K^n over the commutative ring K with non-trivial multiplicative group. We use ideas of Multivariate and Noncommutative Cryptographies, The paper reflects
author's talk at the algebraic conference ''At the End of the Year'' 27.12.2024 (Kyiv, Ukraine, https://sites.google.com/view/aey2023).

The interest to serious algebraic studies was stimulated recently by the research in Post Quantum Cryptography where among 5 core areas there are Multivariate Cryptography and Code - based Cryptography which need serious algebraic cryptography (linear codes, Goppa codes, Reed-Solomon codes used in McElise cryptosystems and etc).

The NIST project since 2017 is concentrated on Public Keys. aimed for the purposes to produce the encryption tools or instruments for the design of digital signatures (see [3], [4] and further references). We has to admit that PQC secure quadratic multivariate rules can serve to create the shortest digital signature procedures. Recall that we have to add to mentioned above two directions of PQC the Hash based cryptography, Isogeny-based cryptography and Lattice based cryptography. We have to notice that all already NIST certified algorithms are not the public keys of Multivariate Cryptography. Quite long standing "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method was rejected due to cryptanalytic studies published in the Proceedings of the Eurocrypt 2021 [3], [5].

Essential part of algebraic PQC outside of the design of Public Keys is formed by various methods of Protocol developments where algebraic efforts are concentrated on Non Commutative Cryptography. In the case of Group-based protocols correspondents (traditionally Alice and Bob) can use protocols with at least two generators which can generate very large Noncommutative group. They can use semigroups instead of groups to elaborate the collision element g from the semigroup. The case when $\boldsymbol{g}$ is an element of affine Cremona semigroup ${}^nCS(K)$ of all endomorphisms of multivariate ring $K[x_1, x_2..., x_n]$ over the finite commutative K can be useful in Multivariate Cryptography**.**

We refer to the piece of information T as a *trapdoor accelerator* of the elements $\boldsymbol{\sigma}$ of degree $\boldsymbol{2}$ from ${}^nCS(K)$ if the knowledge of T allows to compute the reimage of σ acting on K^n in time $\boldsymbol{O(n^3)}$ (see [38]). In the Section 2 we present the algorithm to use the collision maps of several sessions of secure protocol of Noncommutative Cryptography implemented with the platform-semigroup ${}^nES(K)$ of Eulerian transformation for the save delivery of quadratic endomorphism of $K[x_1, x_2..., x_n]$ from one correspondent to another one. We use this procedure to define protocol based algorithm to make digital signatures.

In Section 3 we discuss the group of Eulerian transformations ${}^nEG(K)$ acting bijectively on the variety $(K^*)^n$ (subsection 3.1). It can be used to make digital signatures. In the subsection 3.2 we consider the protocol based cryptosystem with the platform ${}^nES(K)$ and encryption tool from ${}^nEG(K)$. Both schemes use private information which is the hidden -decomposition of the element into its product into Jordan-Gauss transformations. Schemes 3.1 and 3.2 can be used to make digital signatures In the subsections 3.3 and 3.4 we combine procedure of section 1 for the safe

delivery of quadratic multivariate transformation with the similar procedure for delivery of Eulerian transformation to define two different asymmetric cryptosystems with the space of plaintexts $(K^*)^n$ and the space of ciphertexts K^n**.**
In unit 3.5 we mention the idea of a public key obtained as composition of Eulerian transformation and multivariate transformation of K^n.

For readers convenience section 4 contains description ofthe simplest version of hidden tame homomorphism protocol defined for the semigroups ${}^nES(K)$ and their parabolic subgroups. More general version with ring extensions is described in [12] together with some other ${}^nES(K)$-based protocols.

Section 5 is dedicated to discussions of sources of trapdoor accelerators of quadratic endomorphisms. They include the list of historical cryptosystems over finite fields for which corresponding cryptanalysis was discovered and recent constructions of trapdoor accelerators define over general commutative ring with unity. Section 6 is the Conclusion.

2. Special endomorphisms of $K[x_1, x_2\ldots, x_n]$ and cryptosystems of Post Quantum Cryptography.

2.1 Some definitions.

Task of Affine Cremona Semigroup ${}^nCS(K)$ is defined as endomorphism group of polynomial ring $K[x_1, x_2,..., x_n]$ over the commutative ring K. It is an important object of Algebraic Geometry (see Max Noether paper ''Luigi Cremona'' [34] about Mathematics of Luigi Cremona who was the prominent figure in Algebraic Geometry in the XIX century**, [35]** and further references on papers which use the term *affine Cremona group*). Element of the semigroup σ can be given via its values on variables, i. e. as the rule $x_i \rightarrow f_i(x_1, x_2, \ldots, x_n)$, $i=1, 2,\ldots, n$. This rule induces the map $\sigma': (a_1, a_2,.., a_n) \rightarrow (f_1(a_1, a_2,.., a_n), f_2(x_1, x_2, \ldots, x_n),\ldots, f_n(x_1, x_2,\ldots, x_n))$ on the free module K^n. Automorphisms of $K[x_1, x_2,..., x_n]$ form affine Cremona Group ${}^nCG(K)$. In the case when K is a finite field or arithmetic ring Z_m of residues modulo m elements of affine Cremona Groups or Semigroups are used in algorithms of Multivariate Cryptography. Recall that we refer to the piece of information T as a *trapdoor accelerator* of the elements σ of degree *2* the knowledge of if the knowledge of $\boldsymbol{T}$ allows to compute the reimage of σ' in time $O(n^3)$ **(**see [38]). In this direction of PQC (Post Quantum Cryptography) we use to keep elements $f_i(x_1, x_2, \ldots, x_n)$ of in their standard forms, i. e. lists of their monomial terms ordered lexicographically.

In fact the pair (σ, T) such that the reimage of σ is not computable in polynomial time can be used as public key. Alice has the whole pair (σ, T) but Bob has only the standard form of σ.

If $\boldsymbol{\sigma}$ is an automorphism then it acts bijectively on the space of plaintexts K^n it can be used as encryption tool. Bob encrypts in time $O(n^3)$. The knowledge of T allows Alice to decrypt.

The *public key (σ, T)* can be used as an instrument for digital signatures accordingly to the following scheme. Assume that Alice has *(F, T)* and public user Bob poses *F*.

Let us assume that Alice and Bob use some symmetric cipher *H* and the hash function *f*. Bob receives encrypted by Alice document $H(p)=c$. Correspondents compute ''compressed'' message $f(c)=b$.

Alice considers the equation $F(y)=b$**.** She uses her knowledge on *T* and reconstruct some reimage *r* of ***b*.**

Finally Alice sends *r* to Bob. He is checking the relation $\boldsymbol{F(r)=b}$**.** So Bob is sure that the decrypted by him document ***p*** was genuine and was sent to him by Alice.

Assume that we want to use subsemigroups S_n of ${}^nCS(K)$ for the design of protocols.

Then we have to look at S_n such the following *multiple composition property* (MCP) holds.

Given elements ${}^1s, {}^2s, \ldots {}^ns$ we are able to compute their composition in polynomial time.

Affine Cremona group ${}^nCS(K)$ does not poses MCP. If one takes ***n*** quadratic elements is randomly their product with the probability close to 1 will have degree $\boldsymbol{2^n}$**.**

So the computation is not feasible.

EXAMPLE. Let us assume that we have secure protocol with the collision element ***G***

$$x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \ldots x_n^{a(1,n)},$$
$$x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \ldots x_n^{a(2,n)}, \quad (1)$$
$$\ldots$$
$$x_m \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \ldots x_n^{a(n,n)}$$

where μ_i are regular elements of finite commutative ring *K* with the unity.

It is easy to see that the complexity of the composition of two elements of kind (1) is $O(n^3)$.

We consider the protocol based on computation of $O(1)$ compositions of elements from the semigroup. So the complexity of protocol is $O(n^3)$.

Such a protocol is based on the complexity of finding the decomposition of the transformation (1) into the composition of given generators is presented in [12].

The reprint [36] with this protocol description was posted on IACR e-print archive 5 years ago, see [37] where some of its applications were described.

2.2 Quadratic map delivery procedure.

Assume that *K* is a commutative ring with the nontrivial multiplicative group ($K=F_q$, $q>2$ or $K=Z_m$, $m>2$ are practical cases). So μ_i are elements of ***K*, a(i,j)*** are elements of Z_d, where *d* is the order of the multiplicative group *K**. Alice can form a matrix $b(i,j)=(\mu_i\mu_j)^{a(i,j)}$.

Alice can form the multivariate polynomial expression

$$g=\sum_{i=1,2,\ldots,n}\sum_{j=1,2,\ldots,n} b(i,j)y_iy_j+\mu_1y_1+\mu_2y_2+\ldots+\mu_ny_n+b(n,n) \quad (1)$$

The complexity of computation of *g* is $O(n^2)$.

If Alice and Bob conducts *m*, $m=O(n)$ independent sessions and get outputs with coefficients ${}^k\mu_j$, $k=1,2,\ldots m$, $j=1, 2,\ldots,n$, ${}^ka(i,j)$.

They can form polynomials ${}^kg(y_1, y_2, \ldots, y_n)$, $k=1, 2,\ldots,m$ in time $\boldsymbol{O(n^3)}$**.**

Recall that the cost of single protocol is $O(n^3)$. So the total cost of forming the tuple $({}^1g, {}^2g,\ldots, {}^mg)$ is $O(n^4)$.

Alice can take some multivariate rule F given via the list of polynomials ${}^kf(y_1, y_2, \ldots, y_n)$, $k=1, 2,\ldots, m$ for which Alice knows polynomial invertor T, i. e the piece of information such that the knowledge about $\boldsymbol{T}$ allows her to compute the reimages of F in polynomial time.

Alice sends expressions ${}^kh={}^kg+{}^kf$, $k=1,2,\ldots,m$ written in their standard forms (lists of monomial terms ordered lexicographically) to her trusted partner Bob.

Bob can use form F to make digital signatures or encrypt messages $(p_1, p_2, \ldots, p_n)$ in the case $n=m$ and bjective $\boldsymbol{F}$ for $d=n^2/3$ (or n^2a, $0<a<1/2$) documents or messages. After that Alice and Bob makes a new session of protocol and use changed quadratic form F'. If they will make sessions periodically then adversary is not able to restore $\boldsymbol{F}$ which has $1/2n^2m$ coefficients in its standard form.

Adversary will have dm quadratic equations with $1/2n^2m$ variables in the case when he/she intercepts all messages. Of kind image, reimage. It is not enough to compute the standard form of F and attack the problem of finding its reimages.

They can use for instance "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method for the generation of $F, F', F'', \ldots$.

In terms of algebraic cryptography a post-quantum secure procedure for the electronic signature of $O(n^t)$, $t \geq 1$ documents is defined where n is the number of variables of temporarily used multivariate rule (size of the signature) is executed in time $O(n^{3+t})$. This is the best known time for the completion of this mass problem. The security of the procedure is based on the secure protocol of Non-Commutative Cryptography on the platform of Eulerian transformations of the set $(K^*)^n$. Noteworthy that signing of $O(n^t)$, $t<1$ takes time $O(n^4)$ because of the cost of the protocol with $O(n)$ outputs.

REMARK 1. *Secure classical quadratic multivariate rule with n variables will allow to sign* $\boldsymbol{O(n^t)}$, $\boldsymbol{t\geq 0}$ *documents in time* $O(n^{3+t})$.

REMARK 2 (on ***(F, T))*** **.** *The method works in the case of arbitrary commutative ring K with nontrivial multiplicative group K*.*

We construct the method of construction of quadratic automorphism from ${}^nCS(K)$ with the trapdoor accelerator for each pair (K, n) (see abstract of the conference [58] or [1] were the prove of this result can be found). Hope that multivariate cryptographic K-theory can bring interesting for cryptanalysts examples of public key candidates and protocol based cryptosystems.

2.3 On multiple usage of delivery procedure.

Correspondents can take positive integer m, $m=O(1)$, $m \geq 2$ and execute the following procedure **of** secure delivery of $\boldsymbol{m}$ multivariate rules ${}^iF \in {}^nCS(K)$ given by ${}^jF(y_i) = {}^jf_i(y_1, y_2,\ldots, y_n)$, $j=1,2,\ldots m$, $i=1,2,\ldots, n$.

Let ${}^1h, {}^2h,\ldots, {}^{mn}h$ is the list of ${}^jf_i$ ordered lexicographically. Alice and Bob execute the protocol mn times and form the expression ${}^sg(y_1, y_2, \ldots y_n)$, $s=1, 2, \ldots, ml$. So Alice sends ${}^ih+{}^ig$ via an open channel. So Bob gets maps ${}^iF$, $i=1,2, \ldots m$

Option 1.

For the establishment of digital signature procedure Alice selects ${}^iF$, $i=1,2, \dots n$ as the maps with the trapdoor accelerators ${}^iT$. She may check that the degree of composition of selected maps is 2^m.

Bob takes the hash value $c=(c_1, c_2, \dots, c_n)$ of the encrypted document. The knowledge of trapdoor accelerators allows Alice to compute recursively reimages ${}^1c=({}^mF)^{-1}(c)$, ${}^2c=({}^{m-1}F)^{-1}({}^1c), \dots, {}^mc==({}^1F)^{-1}({}^{m-1}c)=(p_1, p_2, \dots, p_n)=p$.

She sends p via an open channel.

Bob computes ${}^1p={}^1F(p), {}^2p={}^2F({}^1p), \dots, {}^mp={}^mF({}^{m-1}p)$.

In the case of coincidence of ${}^mp$ with c Bob knows that he gets the genuine document from Alice.

Correspondents can execute this digital signature procedure up to $r=1/3n^d$, $d=2^m$, $m=0(1)$ and use parameter r as the period of repetition of protocol sessions.

The cost of signature of $O(n^t)$, $1< t<d$ documents will be $O(n^{t+3})$ with the usage of a single session of the protocol. Alice and Bob can use the same length of digital signatures as in the procedure with multivariate quadratic public keys.

Option 2.

Alice and Bob use the previous procedure (option 1) with parameter $m=O(\log_2(n))$.

The cost of protocol in tis case is $O(n^4\log_2(n))$

Then the composition F of ${}^iF$ has a linear degree as the function from n.

In this case after the execution of the prococol the cost of signature of single document will be $O(n^3\log_2(n))$. So n^t, $t>1$ documents will be signed in time $O(n^{t+3}\log_2 n)$.

Option 3.

Let $\{z(1), z(2), \dots, z(m)\}=Z$, $m=O(1)$, $m>1$ be the formal alphabet. Correspondents use the option to write nonempty word $w=z(i(1)zi(2), \dots, z\_(i(l), l=O(1), l>0$ where $i(1), i(2), \dots, i(l)$ are elements of $\{1,2,\dots,m\}$ and work with specialisation ${}^{i(1)}F\,{}^{i(2)}F\dots{}^{i(l)}F=F(w)$ (the composition of maps). Bob computes the value of F(w) iteratively via the consecutive application of ${}^{i(s)}F$, $s=1,2,\dots,m$. Alice is able to compute the reimage of $F(w)$ because she knows trapdoor accelerators. The word w is agreed via an open channel.

Alice and Bob are able to use single word up to $1/3n^2$ times.

Correspondents can use this option during practically unlimited period.

Of course they can change generators ${}^iF$ via the new protocol session.

3. Eulerian transformations and asymmetric cryptosystems.

3.1. On the group of Eulerian transformations.

Let ${}^nES(K)$ stands for the semigroup of all endomorphisms of $K[x_1, x_2, \dots, x_n]$ of kind ***(1)*** where K be a finite commutative ring with the multiplicative group K^* of regular elements of the ring. We consider the action of Eulerian semigroup ${}^nES(K)$ of transformation of kind

$x_1 \longrightarrow \mu_1 x_1^{\,a(1,1)} x_2^{\,a(1,2)} \dots x_n^{\,a(1,n)}$,

$x_2 \longrightarrow \mu_2 x_1^{\,a(2,1)} x_2^{\,a(2,2)} \dots x_n^{\,a(2,n)}$,

…

$X_n \to M_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)}$,

where $a(i,j)$ are elements of arithmetic ring Z_d, $d=|K^*|$, $M_i \in K^*$ on the set ${}^nE(K) = (K^*)^n$. Let ${}^nEG(K)$ stand for Eulerian group of invertible transformations from ${}^nES(K)$. They act as bijective maps on the variety $(K^*)^n$.

We can use the following method of generating of invertible elements.

Let π and δ be two permutations on the set $\{1,2,\dots, n\}$. Let us consider a transformation of $(K^*)^n$, $d = |K^*|$. (the most important cases are $K=Z_m$ or $K= F_q$). We define transformation ${}^AJG(\pi, \delta)$, where A is triangular matrix with positive integer entries $0 \le a(i,j) \le d$, $i \ge j$ defined by the following closed formula.

$y_{\pi(1)} = M_1 x_{\delta(1)}^{a(1,1)}$

$y_{\pi(2)} = M_2 x_{\delta(1)}^{a(2,1)} x_{\delta(2)}^{a(2,2)}$

…

$y_{\pi(n)} = M_n x_{\delta(1)}^{a(n,1)} x_{\delta(2)}^{a(n,2)} \dots x_{\delta(n)}^{a(n,n)}$

where $(a(1,1),d)=1$, $(a(2,2),d)=1, \dots, (a(n,n),d)=1$.

We refer to ${}^AJG(\pi, \delta)$ as Jordan - Gauss multiplicative transformation or simply JG element. It is an invertible element of ${}^nES(K)$ with the inverse of kind ${}^BJG(\delta, \pi)$ such that $a(i,i)b(i,i)=1 \pmod d$. Notice that in the case $K= Z_m$ straightforward process of computation of the inverse of JG element is connected with the factorization problem of integer m.

So Alice can generate g and h as a product of several Jordan Gauss transformations. The simplest case in a spirit of LU factorization is the composition of lower and upper triangular transformations.

The cryptosystem is the following procedure.

Alice can select several Jordan-Gauss transformations $J_1, J_2, \dots, J_d$, $d>1$ from ${}^mEG(K)$ and compute their product J

She can use $\boldsymbol{J}$ *as a public rule.*

Public user works with the space of plaintexts $(K^*)^m$.

He writes his message $(p)=(p_1, p_2, \dots, p_m)$ and form the ciphertext $(c_1, c_2, \dots, c_m)$ as $J(p)$. The knowledge of the decomposition of J into the generators J_i allows her to decrypt.

REMARK. *Adversary has solve the equation $J(x)=c$. The polynomial algorithm to solve this general problem with the use of deterministic machine together with Quantum Computer is not known. Hope that this public key algorithm attracts attention of Cryptanalysts.*

It can be used as digital signatures instrument, The length of signature n can be the same with the case of quadratic multivariate map. The theoretical cost of the execution of the procedure for one document is $O(n^2)$.

It is better estimation then in the case of quadratic multivariate rule.

3.2. Protocol based cryptosystem.

Alice and Bob conduct already mentioned protocol and elaborate the collision element C from the ${}^mES(K)$.

She compute the product of monomials $J(x_i)C(x_i)$, $i=1,2,\dots,m$ and sends it to Bob.

Bob uses J to encrypt his plaintext $(p_1, p_2,..., p_m)$ from $(K^*)^m$. Alice decrypts the ciphertext $(J(p_1), J(p_2),..., J(p_m))$ because her knowledge on the decomposition of J into J_i.

To prevent the linearization attacks by the Adversary Alice has to sign just an, $a<1$ documents after that Alice and Bob repeat the protocol. In fact they use protocol periodically with the period $\boldsymbol{an}$. It allows her to sign in a secure way $O(n^t)$, $t\geq 1$ documents of size n within time $O(n^{2+t})$.

For $O(n^t)$ documents with $t<1$ is required $O(n^3)$ elementary operations. This algorithm has advantage in the comparison with the quadratic public key of Multivariate Cryptography in the case of $O(n^t)$, $0<t<1$ documents. It requires time $O(n^3)$ but not $O(n^{3+t})$.

Option of multiple generators from $^nES(K)$.

Like in the case of the Option 1 of the Section 2 correspondents can use multiple session of protocol to elaborate several elements $^1C, ^2C,..., ^mC$ where $m=0(1)$. It costs time $O(n^3)$. Alice constructs elements ^jJ, $j=1, 2,...m$
as products of several Jordan-Gauss elements. They use the formal alphabet
$\{z(1), z(2), ..., z(m)\} = Z$ to agree on the word $w=z(i(1)z\_\{i(2), ..., z\_(i(l), l=O(1)$, $l>0$ where $i(1), i(2),..., i(l)$ are elements of $\{1,2,...,m\}$. Bob uses specialisation $J(w)= {}^{i(1)}J\, {}^{i(2)}J...{}^{i(l)}J$ for signatures verification. Alice can compute reimages of $J(w)$ because she knows the decompositions of ^jJ, $j=1, 2,...m$ into Jordan-Gauss generators.They can use single word up to $1/2n$ times.
The complexity of signing $O(n^t)$, $t>1$ documents is $O(n^{t+2})$.

3. 3 Combined cryptosystem.

We start of algorithms (1) and (3) with one session of protocol with $\boldsymbol{n+1}$ outputs.

They elaborate collision maps $^1C, ^2C, ..., ^{n+1}C$.

Alice takes bijective quadratic rule $F=G_1$ given by $^kf(y_1, y_2,..., y_n)$ with the corresponding trapdoor accelerator T.

Alice and Bob form $^kg(y_1, y_2,..., y_n)$, $k=1, 2,...,n$ *accordingly to the* described above procedure for $^1C, ^2C, ..., ^nC$.. She sends $^kg(y_1, y_2,..., y_n)+ {}^kf(y_1, y_2,..., y_n)$ to Bob.

Additionally Alice forms invertible transformation $J= G_2$ from $^nEG(K)$ obtained as a product of several Jordan Gauss transformations and sends the products $J(y_i)$ $\boldsymbol{^{n+1}C(y_i)}$ *(monomials)* to Bob.

He restores $J= G_2$ and $F=G_1$. Assume that he uses them for the encryption process. Bob uses combined encryption which transforms open text $\boldsymbol{(x)}$ from $(K^*)^n$ into the ciphertext $\boldsymbol{G_1(G_2(x))}$ from the affine space $(K)^n$. Alice has trapdoor accelerator T and the knowledge on the decomposition of J into Jordan -Gauss generators for the computation of reimages of G_1 and G_2. So Alice decrypts .

The complexity of Bob's encryption of $O(n^t)$, $t\geq 1$ plaintexts is $O(n^{t+3})$. In the case when the quantity of documents $O(n^t)$, $t<1$ the complexity will be $O(n^4)$. The composition of G_1, G_2 has polynomial degree cn, $n>0$ and the density dn^3 , $d>0$. That is why successful linearisation attacks on this cryptosystem are not feasible in a polynomial time. One of the protocol session is sufficient, no need to use periodical sessions.

3.4. **Modified algorithm.**

Alice has the following option to hide the map F from Bob.
She can compute the composition H of $J=G_2$ and $F=G_1$. This endomorphism will have a density $O(n^3)$ (number of monomial terms) and degree cn.
Additionally Alice will compute the composition Z of ${}^{n+1}C$ and G sending x_i to $G(x_1)={}^{i}g(x_1, x_2, \dots, x_n)$, $i=1,2,\dots,n$.

She sends $Z(x_i)+H(x_i)$ to Bob.

He restores the map H and uses it for the encryption of plaintexts from $(K^*)^n$.
Encryption by Bob takes time $O(n^4)$.

Alice can decrypt because of her knowledge about the polynomial invertor T and decomposition of J into Gauss-Jordan generators.

3.5. **Some public keys.** Without usage of the protocol Alice creates G_1 (quadratic or cubic) and G_2 computes the standard form $H=G_1(G_2)$ and announce it as a public rule. Such public keys were a suggested in 2017 ([56], [57]).

During the period more than 6.5 years instruments to break these public keys are not discovered.

3.6. Option of multiple Eulerian and quadratic generators.

We suggest generalisation of algorithm 3.3 with several Eulerian transformations ${}^1J, {}^2J,\dots, {}^lJ$, $l=O(1)$ and several quadratic transformations ${}^1F, {}^2F,\dots, {}^mF$, $m=O(1)$. Alice can use several protocols with Bob and safely deliver these transformation to Bob in time $O(n^4)$.

Correspondents use two alphabets $\{u_1, u_2, \dots, u_l\}$ and $\{z_1, z_2,\dots, z_m\}$. They agree via open channel on words $w(1)=u_{i(1)}u_{i(2)}\dots u_{i(s)}$, $s>0$, $s=O(1)$, $i(k)\in\{1,2,\dots, l\}$ and $w(2)=z_{j(1)}z_{j(2)}\dots z_{j(d)}$, $d=O(1)$, $d>0$ where $j(1), j(2),\dots, j(d)$ are elements of $\{1,2,\dots,m\}$ and work with specialisations ${}^{i(1)}J\ {}^{i(2)}J\dots{}^{i(s)}J=J(w(1))$ and ${}^{i(1)}F\ {}^{i(2)}F\dots{}^{i(d)}F=F(w(2))$.

To encrypt Bob consecutively applies ${}^{i(1)}J, {}^{i(2)}J, \dots, {}^{i(s)}J$ to his plaintext $p\in(K^*)^n$ and gets $u\in(K^*)^n$. Secondly he applies consecutively ${}^{(1)}F, {}^{i(2)}F,\dots, {}^{i(d)}F$ to u and gets ciphertext $c\in K^n$.

Alice can decrypt because of her knowledge on trapdoor accelerators of ${}^jF$ and decompositions of ${}^iJ$ into products of Jordan-Gauss decompositions. They can use selected pair $w(1),w(2)$ safely up to $1/3n^2$ times.

3.7 Option with single Eulerian transformation and multiple quadratic maps.

We can use previous scheme 3.6 with $l=1$ and $m=O(\log_2(n))$.

The protocol for the delivery of ${}^1J$ and ${}^1F, {}^2F,\dots, {}^mF$, $m=c\log_2(n)$ from Alice to Bob will cost time $O(n^4\log_2(n))$.

Alice constructs ${}^1J$ as a product of $O(1)$ Jordan-Gauss transformations. She selects quadratic maps ${}^1F, {}^2F,\dots, {}^mF$ with the trapdoor accelerators.

Bob encrypts his message (p) from $(K^*)^n$ via the consecutive application of ${}^1J$, ${}^1F$, ${}^2F,\ldots,{}^mF$. It takes him time $O(n^3 log_2(n))$. Alice decrypts because of her knowledge on the trapdoor accelerators of ${}^iF$ and the decomposition of ${}^1J$ into the Jordan-Gauss elements.

4. Hidden tame homomorphism protocols on platforms of special multivariate transformations.

4.1. Abstract scheme.

The following abstract scheme can be used (see [20]). Assume that there are two families of subsemigroups $E_n(K)$ and $L_n(K)$ of ${}^nCS(K)$ $(E_n(K)>L_n(K))$ together with two families $E'_m(K)$ and $M_m(K)$ of subsemigroups ${}^mSC(K)$ $(E'_m(K)>M_m(K))$ such that $n>m$, $m=O(n)$ and there is a feasible homomorphism ψ from $L_n(K)$ into $M_m(K)$ (computable in time $O(n^k)$).
We assume that $E_n(K)$ and $E'_m(K)$ has rather large subgroups of invertible elements.

Alice and Bob can execute the following protocol

Alice selects generators $g_1, g_2, \ldots, g_d$, $d\geq 2$ from $L_n(K)$ and the invertible elements $\boldsymbol{g}$ and $\boldsymbol{h}$ from $E_n(K)$ and $E'_m(K)$ respectively.
She computes images $h_1=\psi(g_1)$, $h_2=\psi(g_2),\ldots, h_d=\psi(g_d)$. After that Alice computes- $(a_i=gg_ig^{-1}, b_i=hh_ih^{-1})$, $i=1,2,\ldots,d$ and sends it to his partner Bob via open channel.

He take an alphabet $z_1, z_2, \ldots, z_d$ and writes the word
$z_{i(1)}z_{i(2)}\ldots z_{i(l)}$ of the length $l=O(1)$, $l>d$, $i(1), i(2),\ldots, i(l)$ are elements from $\{1,2,\ldots,d\}$. Bob computes the standard form of $a=a_{i(1)}a_{i(2)}\ldots a_{i(l)}$ and sends it to Alice. He computes $b= b_{i(1)}b_{i(2)}\ldots b_{i(l)}$ and keeps it for himself.
Alice computes the collision element $\boldsymbol{b}$ accordingly to the following procedure.
*1)*She computes $g^{-1}ag={}^1g$ *2)* she gets the standard form of $\psi({}^1g)={}^2g$ *3)* computes b as $h({}^2g)h^{-1}$.
The adversary has to decompose of a in its standard form into the word $w(a_1, a_2, \ldots, a_d)$ of given generators $a_1, a_2, \ldots, a_d$. If he/she solves this ***NP***-hard problem then the adversary has the collision element as $w(b_1, b_2, \ldots, b_d)$.

4.2. The implementation with Eulerian transformation.

Let K be a finite commutative ring with the multiplicative group K^* of regular elements of the ring. We take Cartesian power ${}^nE(K)=(K^*)^n$ and consider an Eulerian semigroup ${}^nES(K)$ of transformations of kind

Let ${}^nEG(K)$ stand for Eulerian group of invertible transformations from ${}^nES(K)$. They act as bijective maps on the variety $(K^*)^n$.

Let $J=\{1, 2,\ldots,m\}$ we consider totality ${}^mP_n(K)$ of all transformation of kind

$x_1 \longrightarrow M_1 x_1^{\,a(1,1)} x_2^{\,a(1,2)} \dots x_m^{\,a(1,m)}$
$x_2 \longrightarrow M_2 x_1^{\,a(2,1)} x_2^{\,a(2,2)} \dots x_m^{\,a(2,m)}$
$\dots$
$x_m \longrightarrow M_m x_1^{\,a(m,1)} x_2^{\,a(m,2)} \dots x_m^{\,a(m,m)}$
$x_{m+1} \longrightarrow M_{m+1} x_1^{\,a(m+1,1)} x_2^{\,a(m+1,2)} \dots x_m^{\,a(m+1,m)} x_{m+1}^{\,a(m+1,m)} \dots x_n^{\,a(m+1,n)}$
$x_{m+2} \longrightarrow M_{m+2} x_1^{\,a(m+2,1)} x_2^{\,a(m+2,2)} \dots x_m^{\,a(m+2,m)} x_{m+1}^{\,a(m+2,m)} \dots x_n^{\,a(m+2,n)}$
$\dots\dots$

$x_n \longrightarrow M_n x_1^{\,a(n,1)} x_2^{\,a(n,2)} \dots x_m^{\,a(n,m)} x_{m+1}^{\,a(n,m+1)} \dots x_n^{\,a(n,n)}$

Let $\psi: {}^mP_n(K) \rightarrow {}^mES(K)$ be the homomorphism sending σ from ${}^mP_n(K)$ into its restriction onto $K[x_1, x_2, \dots, x_m]$.

We can use described above protocol in the case of $E_n(K) = {}^nES(K)$, $L_n(K) = {}^mP_n(K)$ and $E'_m(K) = M_m(K) = {}^mES(K)$.

.Alice and Bob conduct the protocol and elaborate the collision element C from the ${}^mEG(K)$.

5. On the sources of trapdoor accelerators.

5.1. Historical cryptosystems defined over finite fields.

The major stream of Multivariate Cryptography is a search for pairs (F,T) forming the quadratic or cubic trapdoor accelerator where F is the transformation of the vector space defined over the finite field. Developers were hoped that the recovery of the reimage of F given in its standard form without a knowledge of T will stay as unsolved NP-hard problem. The fact that quadratic transformations of public key (F,T) can provide the shortest known digital signatures is motivating a further search for appropriate trapdoor accelerators.
This search was started by Imai and Matsumoto [39] (see also [24]) who constructed a trapdoor accelerator in the case of finite fields of characteristic *2*. They use quadratic extensions F_2 of a finite field $F_1 = F_q$, $q = 2^m$ of characteristics *2* of degree n. They expressed a bijective transformation of F_r, $r = q^n$ of kind $x \rightarrow x^t$, $t = q^a + 1$ where $(a+1, q^r - 1) = 1$ as quadratic transformation F of the vector space $(F_1)^n$. Authors suggested to use the standard form $G = L_1 F L_2$ where L_1 and L_2 are elements of $AGL_n(F_1)$ as the public rule corresponding to trapdoor accelerator (G, T), $T = (L_1, L_2, a)$.

The cryptanalytic tools to break this potential cryptosystem were found by J. Patarin (see [10] and further references).
Long history of various modifications of Imai-Matsumoto cryptosystems is partially reflected in [23] or [7] . All of them were broken via corresponding cryptanalytic tools. We just mentioned some other cryptosystems inclusive Hidden Fields Equations suggested by J. Patarin and recent Unbalanced Oil and Vinegar cryptosystem for which corresponding cryptanalysis can be found in [5]. This search is continue. We believe in a future success of this direction. Incomplete list of publication with multivariate constructions surveys and cryptanalytic studies is [4], [5], [9], [15], [16],

[17], [18], [19], [40]-[52] . We contributed description of two different families of quadratic cryptosystems [8], [13]-[14].
Recall that we suggest to combine former or current candidate to quadratic
Multivariate public rules with the protocol of Noncommutative Cryptography implemented with the platform of Eulerian transformation of the variety $(F_q)^n$.

5. 2-Stable semigroups over general commutative ring and alternating protocol.

We say that subsemigroup S is k-stable if the maximal degree of its representative equals k, $k>0$.
As it follows instantly from the definition k-stable S poses MCP property.
Examples of such subsemigroup are constructed in the cases of arbitrary k and arbitrary commutative ring K.
We can slightly modify previous protocol in the case when subgroups $E_n(K)$ and $E'_m(K)$ are 2-stable.
Recall that we have two families of subsemigroups $E_n(K)$ and $L_n(K)$ of ${}^nCS(K)$ $(E_n(K)>L_n(K))$ together with two families
$E'_m(K)$ and $M_m(K)$ of subsemigroups ${}^mSC(K)$ $(E'_m(K)>M_m(K))$ such that $n>m$, $m=O(n)$ and there is a feasible homomorphism ψ from $L_n(K)$ into $M_m(K)$ (computable in time $O(n^k)$).
Alice and Bob can execute the following protocol .
Alice selects generators $g_1, g_2, \ldots, g_d$, $d\geq 2$ from $L_n(K)$ and the invertible elements g and h from $E_n(K)$ and $E'_m(K)$ respectively. Additionally she take l_1 from $AGL_n(K)$ and l_2 from $AGL_m(K)$.
She computes images $h_1=\psi(g_1)$, $h_2=\psi(g_2), \ldots, h_d=\psi(g_d)$. After that Alice computes
$(a_i=l_1 g g_i g^{-1} l_1^{-1}$, $b_i=l_2 h h_i h^{-1} l_2^{-1})$, $i=1,2,\ldots, d$ and sends it to his partner Bob via open channel.
Bob conducts the same steps as in the previous algorithm,
Alice computes the collision map b with almost the same procedure. She need just to change conjugators g an h on $l_1 g$ and $l_2 h$.
This protocol can be used for the delivery multivariate rule F from Alice to Bob. Alice (or Bob) sends $F+b$ to her (his) partner.
Noteworthy that the costs of this protocol is $O(n^7)$.
So the usage of transported F *with the trapdoor accelerator for the encryption of* $O(n^t)$, $0<t<2$ *costs* $O(n^7)$. *Correspondents can use this quite expensive scheme to sign important documents. The period of usage has to be* an^2, $0<a<1/2$.
In [8] (see also [1]) we propose a new family of large nonlinear platforms of Noncommutative Cryptography which is a subsemigroups ${}^{m,k}C_n(K)$, $n>k>m>0$ of ${}^{m(n-m)}CS(K)$ formed by the elements of degree ≤ 2. There is a homomorphism of this semigroup onto $ASL_{k(n-k)}(K)$ which is a semigroup of all linear transformation of affine space $K^{k(n-k)}$ and has dimension $>k^2(n-k)^2$ as algebraic variety. These constructions generalise previous platforms [20],[21], [22] in terms of Double Schubert Graphs.
Let ${}^{m,k}G_n(K)$ be the subgroup of all automorphisms of $K[x_1, x_2, \ldots, x_{m(n-m)}]$ from ${}^{m,k}C_n(K)$. Then there is a homomorphism **of** ${}^{m,k}G_n(K)$ onto $AGL_{k(n-k)}(K)$.

Proposition. *For each quadratic representative of* ${}^{m,k}C_n(K)$ *a trapdoor accelerator can be constructed.*

Elements from the ${}^{m,k}G_n(K)$ with a trapdoor accelerator can not be used as public key rules because their inverses are also quadratic transformations but they can be used in the protocol based cryptosystems.

In fact large subsets ${}^{m,k}C'_n(K)$, ${}^{m,k}C'_n(K) > {}^{m,k}C_n(K)$ of elements from ${}^{m(n-m)}CS(K)$ with a trapdoor accelerator were constructed in [8],[1]. Elements from ${}^{m,k}C'_n(K) - {}^{m,k}C_n(K)$ are not stable, some of them can be used for the constructions of public keys see [8].

The constructions of other 2 -stable transformation based can on graphs of increasing girth can be found in [13], [14].

Not so economic schemes for digital signature are considered in [53], [54], [55].

6. Conclusion.

Many schemes of Noncommutative Cryptography (see [11], [25]-[33]) are given in terms of abstract groups (or semigroups). Users has to select a family of groups or semigroups which usually are defined in terms of generators and relations . We suggest some schemes in terms of special transformations semigroups which are the subgroups of affine Cremona semigroup forme by endomorphisms of $K[x_1, x_2,\dots, x_n]$ where K is some finite commutative with the nontrivial multiplicative group. To make symbolic computations feasible er require multiple composition property (MCP**)** which insures the computation of n elements from the subsemigroup of $End(K[x_1, x_2,\dots, x_n])$ in a polynomial time.

In this paper we consider an application of this approach to the construction of the digital signatures or encryption schemes with a quadratic multivariate transformation F. We can use mentioned above protocols in terms of polynomial transformations of K^n for secure delivery of standard form F from one correspondent to another**.** Adversary can intercept many pairs of kind *plaintext/ciphertext* or *hashed document/ its signature* and try to reconstruct the map F**.** Alice and Bob can work with periodical sessions of protocols.

So we suggested several cryptosystems which can work with the tuples of size comparable with the length of digital signatures of quadratic multivariate public rule. We expect that some quadratic multivariate public keys will be certified in future while the proposed in this paper secure protocol based cryptosystems currently can serve as encryption schemes or systems for digital signatures.

Funding Information. This research is supported by British Academy Fellowship for Researchers under Risk 2022 and partially supported by British Academy award LTRSF\100333

References

[1] V. Ustimenko, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022, 198 p.

[2] PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates, https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4.

[3] Anne Canteaut, François-Xavier Standaert (Eds.), Eurocrypt 2021, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Tech-niques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839p.
[4] Jintai Ding, Joshua Deaton, Vishakha, and Bo-Yin Yang, The Nested Subset Differential Attack,A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes, In Eurocrypt 2021, Part 1, pp. 329-347.
[5] Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.
[6] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, IACR e-print archive, 2022/1537.
[7] L. Goubin, J. Patarin, Bo-Yin Yang, Multivariate Cryptography, Encyclopedia of Cryptog-raphy and Security, (2nd Ed.) 2011, 824-828.
[8] V. Ustimenko, Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography, IACR e-print archive, 2023/175.
[9] . Ding and A. Petzoldt, "Current State of Multivariate Cryptography," in IEEE Security & Privacy, vol. 15, no. 4, pp. 28-36, 2017, doi: 10.1109/MSP.2017.3151328.
[10] N. Koblitz, Algebraic aspects of cryptography, Springer (1998), 206 p.
[11] Alexei Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryp-tography, Berlin: BirkhäuserVerlag.
[12] V.Ustimenko, On Eulerian semigroups of multivariate transformations and their crypto-graphic applications. European Journal of Mathematics 9, 93 (2023).
[13] Vasyl Usimenko, Aneta Wroblewska, Extremal algebraic graphs, quadratic multivariate public keys and temporal rules, https://eprint.iacr.org/2023/738.pdf .
[14]] Vasyl Ustimenko, Aneta Wróblewska, Extremal algebraic graphs, quadratic multivariate public keys and temporal rules, FedCSIS 2023: 1173-1178.
[15] Smith-Tone, D. (2022), 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes, Proceedings of PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US, [online], https://doi.org/10.1007/978-3-031. 17234-2_10, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935191.
[16] Daniel Smith Tone, New Practical Multivariate Signatures from a Nonlinear Modifier, https://eprint.iacr.org/2021/429.pdf
[17] Daniel Smith-Tone and Cristina Tone, A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code, https://eprint.iacr.org/2019/1355.pdf
[18] Jayashree, Dey, Ratna Dutta, Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions, ACM Computing Survey, volume 55, issue 12,No.246, pp 1-34, https://doi.org/10.1145/3571071.
[19] Ikematsu, Y. , Perlner, R. , Smith-Tone, D. , Takagi, T. and Vates, J. (2018), HFERP -- A New Multi-variate Encryption Scheme, PQCrypto 2018: The Ninth International Conference on Post-Quantum Cryptography, Fort Lauderdale, FL, US, [online], https://doi.org/10.1007/978-3-319-79063-3_19, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=925152.
[20] V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame hommorphism. Dopovidi. NAS of Ukraine, 2018, n 10, pp.26-36.
[21] V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semi-groups of affine Cremona group, Theoretical And Applied Cybersecurity, Vol. 1 No. 1 (2019) https://doi.org/10.20535/tacs.2664-29132019.1.
[22] V. Ustimenko, On computations with Double Schubert Automaton and stable maps of Multivariate Cryptography, Position and Communication Papers of the 16th Conference on Computer Science and Intelligence Systems pp. 123-130 , DOI: 10.15439/2021F67 ISSN 2300-5963 ACSIS, Vol. 26.
[23] Jintai Ding, A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation, https://link.springer.com/content/pdf/10.1007/978-3-540-24632-9_22.pdf , March 2004DOI: 10.1007/978-3-540-24632-9_22 , Conference: Public Key Cryptography - PKC 2004, 7th Internation-al Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004..
[24]] Ding, J., Petzoldt, A., Schmidt, D.S. (2020). The Matsumoto-Imai Cryptosystem. In: Mul-tivariate Public Key Cryptosystems. Advances in Information Security, vol 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3.
[25] J.A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, 2017, vol.16,(08):1750148.
[26] Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryp-tography and Complexity of Group-theoretic Problems, American Math-ematical Society.

[27] Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382.
[28] Myasnikov A., Roman'kov V. A linear decomposition attack // Groups, Complexity, Cryp-tology. 2015. Vol. 7. P. 81–94.
[29] Roman'kov V. A. A nonlinear decomposition attack. Groups, Complexity, Cryptology. 2017. Vol. 8, No. 2. P. 197–207.
[30] Romankov V. Two general schemes of algebraic cryptography. Groups, Complexity, Cryp-tology. 2018. Vol. 10, No. 2. P. 83–98.
[31] Roman'kov V. An improved version of the AAG cryptographic protocol. Groups, Com-plexity, Cryptology. 2019. Vol. 11, No. 1. 1 2.
[32] Tsaban B. Polynomial time solutions of computational problems in noncommutative alge-braic cryptography. Journal of Cryptology. 2015. Vol. 28, No. 3. P. 601–622.
[33] Ben-Zvi A., Kalka A., Tsaban B. Cryptanalysis via algebraic spans. Advances in Cryptology – CRYPTO 2018 / eds.: H. Shachan, A. Boldyreva. Berlin: Springer, 2018. P. 1–20. (LNCS; vol. 109991).
[34] M. Noether, Luigi Cremona, Mathematische Annalen, 59 (1904), pp. 1-19.
[35] Yu. Bodnarchuk, Every regular automorphism of the affine Cremona group is inner, Jour-nal of Pure and Applied Algebra 157 (2001) 115-119.
[36] V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, IACR e-print Archive 2019/133(PDF) 2019/133(PDF)
[37] V. Ustimenko, On affine Cremona semigroups, corresponding protocols of Non-commutative Cryptography and encryption with several nonlinear multivariate transformations on secure Eulerian mode. IACR e-print Archive 019/1130(PDF)
[38] Vasyl Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, IACR e-print archive, 2022/1537.
[39] Matsumoto Tsutomu and Imai Hideki. 1988. Public quadratic polynomial-tuples for effi-cient signature-verification and message-encryption. In Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 419–453.
[40] Cabarcas Daniel, Smith-Tone Daniel, and Verbel Javier A.. 2017. Key recovery attack forZHFE. In International Workshop on Post-Quantum Cryptography.Springer, 289-308.
[41] Cabarcas Felipe, Cabarcas Daniel, and Baena John. 2019. Efficient public-key operation in multivariate schemes. Advances in Mathematics of Communica-tions 13, 2 (2019), 343.
[42] Cartor Ryann, Gipson Ryan, Smith-Tone Daniel, and Vates Jeremy. 2016. On the differen-tial security of the HFEv-signature primitive. In Proceedings of the Post-Quantum Cryptog-raphy. Springer, 162–181.
[43] Cartor Ryann and Smith-Tone Daniel. 2018. EFLASH: A new multivariate encryption scheme. In Proceedings of the International Conference on Selected Areas in Cryptog-raphy. Springer, 281–299.
[44] Casanova Antoine, Faugère Jean-Charles, Macario-Rat Gilles, Patarin Jacques, Perret Lu-dovic, and Ryckeghem Jocelyn. 2017. Gemss: A great multivariate short signa-ture. Submission to NIST (2017).y. Springer, Singapore, 209–229.
[45] Chen Jiahui, Ning Jianting, Ling Jie, Lau Terry Shue Chien, and Wang Yacheng. 2020. A new encryption scheme for multivariate quadratic systems. Theoretical Computer Sci-ence 809 (2020), 372–383.
[46] Chen Ming-Shing, Hülsing Andreas, Rijneveld Joost, Samardjiska Simona, and Schwabe Peter. 2018. SOFIA: MQ-based signatures in the QROM. In Proceedings of the IACR Inter-national Workshop on Public Key Cryptography. Springer, 3–33.
[47] Ding Jintai, Perlner Ray, Petzoldt Albrecht, and Smith-Tone Daniel. 2018. Improved crypta-nalysis of hfev-via projection. In Proceedings of the International Conference on Post-Quantum Cryptography. Springer, 375–395.
[48] Ding Jintai, Petzoldt Albrecht, and Schmidt Dieter S.. 2020. Multivariate Public Key Cryp-tosystems, Second Edition. Advances in Information Security. Springer
[49] Ding Jintai, Zhang Zheng, Deaton Joshua, Schmidt Kurt, and Vishakha F.. 2019. New at-tacks on lifted unbalanced oil vinegar. In Proceedings of the 2nd NIST PQC Standardiza-tion Conference.
[50] Ding Jintai, Zhang Zheng, Deaton Joshua, and Wang Lih-Chung. 2020. A complete crypta-nalysis of the post-quantum multivariate signature scheme Himq-3. In Proceedings of the International Conference on Information and Communications Security.
[51] Dung H. Duong, Ha T. N. Tran, Willy Susilo, and Le Van Luyen. 2021. An efficient multi-variate threshold ring signature scheme. Computer Standards & Interfaces 74.

[52] Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. 2022. A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive (2022).
[53] V. Ustimenko, On Multivariate Algorithms of Digital Signatures of Linear Degree and Low Density. IACR ePrint Archive 2020/1015.
[54] V Ustimenko, On Multivariate Algorithms of Digital Signatures on Secure El Gamal Type Mode. IACR ePrint Archive 2020/984.
[55] V. Ustimenko, On Multivariate Algorithms of Digital Signatures Based on Maps of Unbounded Degree Acting on Secure El Gamal Type Mode. IACR ePrint Archive 2020/1116.
[56] V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, IACR e-print archive.2017/093(PDF)
[57] V. A. Ustimenko. On new multivariate cryptosystems based on hidden Eulerian equations, Dopovidi of National Academy of Science of Ukraine N5, 2017..
[58]] Ustimenko V. On new platforms of Noncommutative Cryptography designed viathe walks on algebraic graph and their applications, Ukraine Algebra Conference At the End of the Year 2023, December 26 27, 2023, book of abstracts, Kyiv, Ukraine, page 53.